Concatenated Shift Registers Generating Maximally Spaced Phase Shifts of PN-Sequences

W. J. Hurd
Communications Systems Research Section

L. R. Welch
University of Southern California

A large class of linearly concatenated shift registers is shown to generate approximately maximally spaced phase shifts of pn-sequences, for use in pseudorandom number generation. A constructive method is presented for finding members of this class, for almost all degrees for which primitive trinomials exist. The sequences which result are not normally characterized by trinomial recursions, which is desirable since trinomial sequences can have some undesirable randomness properties.

I. Introduction

Binary maximal length linear recurring sequences, also known as pn-sequences, m-sequences, or maximal length linear shift register sequences, are known to have good randomness properties and hence are often used in pseudorandom number generation (Refs. 1, 2). Since all different phase shifts of the same sequence are essentially uncorrelated, weighted sums of several different phase shifts are also essentially uncorrelated for distances up to the minimum distance between the component phase shifts. Thus efficient methods for simultaneous generation of several maximally spaced phase shifts of the same pn-sequence are useful in generating pseudorandom numbers.

Various methods have been presented for generating several phase shifts of the same pn-sequence (Refs. 3-7). The major drawback in these techniques is that for high-degree recursions it is computationally infeasible to evaluate the distances between the phase shifts. When the distances are computable or controllable, they are fairly small – at least small enough so that one could operate the generator long enough to see correlations between the phase shifts. Hurd (Ref. 8) has presented a method for generating approximately maximally spaced phase shifts of the product of two pn-sequences, and the autocorrelation properties of such sequences are good (Ref. 9), but the method is more efficient to implement in hardware than in software, and it has the minor disadvantage that the sequence is not quite maximal length.

We present here a large class of efficient algorithms for generating approximately maximally spaced phase shifts of pn-sequences; that is, the phase shifts approximately equipartition the period of the sequence. Second, we present a constructive method for finding an appropriate configuration for almost every degree for which there exists a primitive trinomial. The recursions which result are *not* generally trinomial recursions, which is desirable since some trinomial recursions have less desirable randomness properties than others (Refs. 10-12).

II. Description and Motivation

Figure 1 shows a general linear concatenation of shift registers. The algebraic description is as follows: There are N binary shift registers with lengths $L_0, L_1, \ldots, L_{N-1}$. The content of the ith stage of the kth register at time t is $A_i^k(t)$ and satisfies

$$A_{i+1}^k\,(t+1) = A_i^k(t) \text{ for } 1 \leqslant i < L_k \tag{1}$$

Each register has a linear output function

$$F^k(t) = \sum_{i=1}^{L_k} a_i^k A_i^k(t) \bmod (2) \tag{2}$$

which also serves as the input to the next register:

$$A_1^{k+1}\,(t+1) = F^k\,(t) \quad \text{(superscripts modulo } N\text{)} \tag{3}$$

The sequences $F^k(t)$ satisfy a linear recursion of degree $L = \Sigma\, L_k$.

The output of the generator is the N-tuple $[F^0(t), \ldots, F^{N-1}(t)]$. Alternate outputs are the pseudorandom numbers

$$X(t) = \sum_{k=0}^{N-1} F^k(t) 2^k \tag{4}$$

and

$$Y(t) = \sum_{k=0}^{N-1} F^k(t) \tag{5}$$

where the sums are integer sums (not mod (2)). When the sequence is maximal length, i.e., has period $2^L - 1$, the numbers $X(t)$ and $Y(t)$ are uniformly distributed and binomially distributed, respectively, neglecting the fact that the all zero's N-tuple cannot occur.

The $X(t)$ also have good multidimensional distribution properties. Letting $L_{min} = min\ \{L_0, L_1, \ldots, L_{N-1}\}$ we have:

Theorem I. When the sequence length is $2^L - 1$, $X(t)$ is uniformly distributed and L_{min} consecutive terms are mutually independent (neglecting the effect of the absence of the all-zero bit pattern in the collective register).

Proof: Since a repeat of the collective state of the registers causes a periodic repetition of the output sequence, and since the cycle length is $2^L - 1$, all bit patterns, except all zeros, must occur exactly once in each period. Since the output bits are fed into the next register, the bits in the representation of $[X(t-1), X(t-2), \ldots, X(t-L_{min})]$ are all present in the registers at time t. It follows that $[X(t-1), \ldots, X(t-L_{min})]$ is uniformly distributed in the L_{min}-cube (neglecting the effect of the absence of the all-zero bit pattern).

For the convenience of analysis, an alternate description can be given by defining sequences $A_i^k = [A_i^k(t)\colon\ t \in Z]$ and $F^k = [F^k(t)\colon\ t \in Z]$ and defining a delay operator D on sequence B to be $(DB)(t) = B(t-1)$. With this notation and the implicit assumption that component arithmetic is modulo 2, we have

$$A_1^{k+1} = DF^k \tag{6}$$

and

$$A_i^k = D^{i-1} A_1^k \tag{7}$$

From the definition of F^k,

$$F^k = \sum_{i=1}^{L_k} D^{i-1} a_i^k A_1^k = \left(\sum_{i=1}^{L_k} D^i a_i^k \right) F^{k-1} \tag{8}$$

(Again superscripts of F are taken modulo N.) Letting

$$f_k(D) = \sum_{i=1}^{L_k} D^i a_i^k,$$

we have

$$F^k = f_k\,(D) F^{k-1} \tag{9}$$

or

$$F^k = \left[\prod_{j=1}^{k} f_j\,(D) \right] F^0 \quad \text{for} \quad 0 \leqslant k \leqslant N-1 \tag{10}$$

In addition

$$F^0 = F^{N \bmod N} = \left[\prod_{j=1}^{N} f_j(D) \right] F^0 \tag{11}$$

where $f_N(D) = f_0(D)$. This last equation implies

$$\left[1 + \prod_{j=1}^{N} f_j(D)\right] F^0 = 0 \tag{12}$$

Furthermore, $F^0, F^1, \ldots, F^{N-1}$ also satisfy this last equation. When this equation is expressed as a relation among the terms of F^0, it is seen to be a linear recursion with constant coefficients and the characteristic polynomial is

$$P(x) = 1 + \prod_{j=1}^{N} f_j(x) \tag{13}$$

Of particular interest in this paper is the case where

$$f_k(x) = x^{a_k}[f(x)]^{b_k} \tag{14}$$

We show that these recursions yield approximately maximally spaced phase shifts whenever the characteristic polynomial is primitive. Recursions of this class are easily implemented in N shift registers, interconnected with output functions which are all powers of one function, $f(x)$, plus some pure delays. If all of the powers b_k are unity, then all of the registers are identical except for some pure delays. In the simplest case, the functions are binomial. Such an example is shown in Fig. 2.

III. Analysis

For the configuration shown in Fig. 2, where all of the registers are the same except for the pure delays of a_k, the delay $d(k, k+1)$ from F^k to F^{k+1} is the same for all k, except for the a_k; i.e., it is a_k plus the delay associated with $f(x)$. However, it is not clear what the delay associated with $f(x)$ is, or what the delay is between nonadjacent registers, i.e., from F^k to F^{k+j} where $j \neq 1$. This complication arises because the sum of the delays between adjacent registers need not equal the period, but may be any integer multiple of the period. We show here that all of the delays are approximately $1/b$ times the period, or greater, where $b = \Sigma b_k$.

The polynomial

$$P(x) = 1 + \prod_{k=1}^{N} f_k(x)$$

introduced in the previous section has degree $L = \Sigma L_k$ provided $a^k_{L_k} = 1$ for all k. For good pseudorandom generators it is desirable that $P(x)$ be irreducible and primitive, and we now make that assumption.

Since all F^k satisfy the same recursion and the recursion is primitive, all of the F^k must be time delays of a common sequence F^0. It follows that $X(t)$ and $X(t-\tau)$ cannot be uncorrelated for all $\tau < 2^L - 1$. Whenever τ is the delay between F^k and F^j for some k and j, a component of $X(t)$ will be identical to a component of $X(t-\tau)$. The question arises as to how small the delay between two register outputs can be. The following lemma will allow us to answer that question for certain generators:

Lemma: Let $P(x)$ be an irreducible, primitive polynomial of degree n over $GF(2)$ and let $x^a[f(x)]^b = 1 \bmod [2, P(x)]$, where a and b are relatively prime, positive integers and $a \cdot b < 2^n - 1$. If $[f(x)]^k = x^{c_k} \bmod [2, P(x)]$ with $1 \leqslant k < b$ and $0 \leqslant c_k < 2^n - 1$, then there is an integer r_k with $1 \leqslant r_k < b$ such that

$$\left|c_k - \frac{r_k}{b}(2^n - 1)\right| < a.$$

Proof: Since P is primitive, there exists an $M \in [0, 2^n - 2]$ such that $f(x) = x^M \bmod [2, P(x)]$. Now $1 = x^a[f(x)]^b = x^{a+bM} \bmod [2, P(x)]$ or $a + bM = q(2^n - 1)$ for some integer q. It follows from the assumptions, that $1 \leqslant q$ and b, q are relative prime.

Next, for each k with $1 \leqslant k < b$ define q_k, r_k by

$$kq = q_k b + r_k \qquad 0 \leqslant r_k < b$$

The range of k and the relative primeness of q and b implies $r_k \neq 0$. Now

$$kM = \frac{kq(2^n - 1) - a \cdot k}{b} = \frac{r_k(2^n - 1) - ak}{b} + q_k(2^n - 1)$$

Observing that $x^{c_k} = [f(x)]^k = x^{kM} \bmod [2, P(x)]$ we see that

$$c_k = \frac{r_k(2^n - 1) - ak}{b} \bmod (2^n - 1).$$

Since $1 \leqslant r_k < b$ and $ab < 2^n$

$$c_k = \frac{r_k}{b}(2^n - 1) - \frac{ak}{b}$$

and

$$|c_k - \frac{r_k}{b}(2^n - 1)| < a$$

This lemma can be used to bound the distances between output sequences from concatenated shift registers when the polynomials $f_j(x)$ are all powers of a common polynomial $f(x)$.

Theorem II. Let

$$P(x) = 1 + \prod_{j=1}^{M} x^{a_j}[f(x)]^{b_j},$$

($a_j \geqslant 0, b_j > 0$), be irreducible and primitive. Let

$$b = \sum_{j=1}^{N} b_j$$

and

$$a = \sum_{j=1}^{N} a_j.$$

Then the distance between F^k and F^j $(i \neq j)$ is at least $(2^n - 1)/b - a$.

Proof: The polynomial can be written $P(x) = 1 + x^a[f(x)]^b$. If a and b were not relatively prime, P would not be irreducible. The degree n is $a + b \cdot \deg f \geqslant a + b$, so clearly $a \cdot b < 2^a \cdot 2^b \leqslant 2^n$. Thus the lemma applies and $[f(x)]^k = x^{c_k}$ where

$$|c_k - \frac{r_k}{b}(2^n - 1)| < a.$$

Now

$$F^j = \prod_{m=i+1}^{j} D^{a_m}[f(D)]^{b_m} F^i \quad \text{if} \quad j > i$$

and

$$F^j = \left[\prod_{m=i+1}^{N-1} D^{a_m}[f(D)]^{b_m}\right]$$

$$\left[\prod_{m=0}^{j} D^{a_m}[f(D)]^{b_m} F^i\right] \quad \text{if } j < i$$

In either case

$$F^j = D^l\,[f(D)]^k\,F^i$$

for some (l,k) with $0 \leqslant l \leqslant a$ and $0 \leqslant k < b$. It follows that

$$F^j = D^{l+c_k} F^i = D^{d(i,j)} F^i$$

From the lemma, it follows that

$$d(i,j) \geqslant \frac{2^n - 1}{b} - a$$

Now $d(i,j)$ is the distance *from i* to *j*. The above argument also applies to $d(j,i)$ so that

$$min\ [d(i,j), d(j,i)] \geqslant \frac{2^n - 1}{b} - a$$

IV. A Class of Examples

Let $P(x) = x^n + x^b + 1$ be an irreducible primitive polynomial. In the field $GF(2^n)$, P has a root α. That is $\alpha^n + \alpha^b + 1 = 0$. Let $\beta = \alpha^{-b}$ so that $\alpha^n = (\beta^{-1} + 1)$ or $1 = \alpha^{-n}\,\beta^{-1}$ $(1 + \beta)$. Raising both sides to the power b and substituting β for α^{-b} gives $1 = \beta^{n-b}\,(1 + \beta)^b$. Thus β is a root of $x^a(1 + x)^b + 1$ where $a = n - b$. Since α is primitive, b and n are relatively prime and it follows that a and b are relatively prime. Furthermore, if b is relatively prime to $2^n - 1$ then β is also primitive. Therefore, any concatenated shift register with outputs functions $D^{a_k}(1 + D)^{b_k}$, $0 \leqslant k \leqslant N - 1$, where

$$\sum_{k=0}^{N-1} a_k = a, \quad \sum_{k=0}^{N-1} b_k = b,$$

with b relatively prime to $2^n - 1$, satisfies the conditions of theorems I and II. We therefore have the theorem:

Theorem III. Let $P(x) = 1 + x^b + x^n$ be an irreducible, primitive polynomial with $GCD(b, 2^n - 1) = 1$. Any concatenated shift register with output functions

$$f_k = x^{a_k}(1+x)^{b_k},$$

and output sequences $F_k(t), 0 \leqslant k \leqslant N - 1$, such that

$$\sum_{k=0}^{n-1} a_k = a$$

and

$$\sum_{k=0}^{N-1} b_k = b,$$

has the following properties, neglecting the effect of the all-zero state:

(1) $X(t) = \sum_{k=0}^{N-1} 2^k F^k(t)$ is uniformly distributed.

(2) $X(t - 1), \ldots, X(t - L)$ are mutually independent for $L \leqslant \min_k(a_k + b_k)$.

(3) $X(t)$ and $X(t + \tau)$ are uncorrelated for $1 \leqslant \tau < \frac{2^n - 1}{b} - a$.

We observe that the characteristic polynomial of the recursion P is of the form $P(x) = (1+x)^b x^a + 1$. This is *not* a trinomial unless b is a power of 2.

Almost all primitive trinomials satisfy theorem III, that is, all but those few where b and $2^n - 1$ are not relatively prime. An extensive list of primitive trinomials up to degree 1000 is given by Zierler and Brillhart (Refs. 13, 14).

When b is not a prime, the class of examples, and theorem III, extend to the cases where c divides b, and c is relatively prime to $2^n - 1$. Letting $\beta = \alpha^{-c}$, then β is a root of the primitive polynomial $(1 + x^{b/c})^c\ x^{n-b} + 1$, which can be implemented in a concatenation of c or fewer registers.

V. Computer Implementation

Members of the class of Section IV are easily implemented by computer programs. In these implementations the bits in position k of L_k consecutive computer words are used to represent the kth register. The number of registers equals the number of bits in a computer word.

For example, consider the system derived from the primitive polynomial $x^{159} + x^{34} + 1$ (Ref. 13) and implemented on a 32-bit machine. Since $GCD(34, 2^{159} - 1) = 1$, the above transformation can be applied and gives the primitive polynomial

$$P(x) = 1 + x^{125}(1+x)^{34}$$

Now define

$$f_0(x) = x^3 (1 + x) = x^3 + x^4$$

$$f_1(x) = f_2(x) = x^3 (1 + x)^2 = x^3 + x^5$$

$$f_3(x) = \ldots = f_{31}(x) = x^4 (1 + x) = x^4 + x^5 .$$

Then

$$1 + \prod_{i=0}^{31} f_i(x) = 1 + x^{125}(1+x)^{34} = P(x).$$

Let $M3$ be the computer word with 1's in positions 0, 1 and 2, and 0's elsewhere; let $M4$ be the computer word with 1's in positions 0 and 3 through 31 and 0's elsewhere; and let $M5$ be the computer word with 1's in positions 1 through 31 and 0's elsewhere. Then the following Boolean expression generates consecutive outputs

$$Z = [M3.AND.X(t-3)]\ .XOR.\ [M4.AND.X(t-4)]\ .XOR.$$
$$[M5.AND.X(t-5)]$$

and the new $x(t)$ is a left or right cycle of Z, one place.

References

1. Golomb, S. W., *Shift Register Sequences,* San Francisco, Holden Day, 1967.
2. Tausworthe, R. C., "Random Numbers Generated by Linear Recurrence Modulo Two," *Math. Comp.*, Vol. 19, pp. 201-209, Apr. 1965.
3. Lewis, T. G. and Payne, W. H., "Generalized Feedback Shift Register Pseudorandom Number Algorithm," *J. Assoc. Computing Machinery,* Vol. 20, No. 3, July 1973, pp. 456-468.
4. Davies, A. C., "Delayed Versions of Maximal Length Linear Binary Sequences," *Electronics Letters*, Vol. 1, No. 1, 1965, p. 61.
5. Davies, A. C., "Further Notes on Delayed Version of Linear Binary Sequences," *Electronics Letters*, Vol. 1, No. 7, Sept. 1965, pp. 190-191.
6. Latawiec, K. J., "A New Method of Generation of Shifted Linear Pseudorandom Sequences, *Proc. IEE*, Vol. 121, No. 8, Aug. 1974, pp. 905-906.
7. Hurd, W. J., "Efficient Generation of Statistically Good Pseudonoise by Linearly Interconnected Shift Registers," *IEEE Trans. Comp.,* Vol. C-23, No. 2, Feb. 1974, pp. 146-152.
8. Hurd, W. J., "A Wideband Gaussian Noise Generator Utilizing Simultaneously Generated pn-sequences," *Proc. 5th Hawaii Internat'l Conf. System Sci.,* pp. 168-170, Jan 1972.
9. Maritsas, D. G., "The Autocorrelation Function of the Two Feedback Shift Register Pseudorandom Source," *IEEE Trans. Comp.,* Oct. 1973, pp. 962-964.
10. Lindholm, J. H., "An Analysis of the Pseudo-Randomness Properties of Subsequences on Long n-sequences," *IEEE Trans. Inform. Th.,* Vol. IT-14, pp. 569-576, July 1968.
11. Toothill, J. P. R., Robinson, W. D., and Adams, A.G., "The Runs Up-and-Down Performance of Tausworthe Pseudo-Random Number Generators, *J. ACM*, Vol. 18, No. 3, July 1971, pp. 381-399.
12. Toothill, J. P. R., Robinson, W. D., and Eagle, D. J., "An Asymptotically Random Tauseworthe Sequence," *J. ACM,* Vol. 20, No. 3, July 1973, pp. 469-481.
13. Zierler, N., and Brillhart, J., "On Primitive Trinomials (Mod 2)," Information and Control, Vol. 13, No. 6, Dec. 1968, pp. 541-554.
14. Zierler, N., and Brillhart, J., "On Primitive Trinomials (Mod 2), II," *Inform. Contr.,* Vol. 14, No. 6, June 1969, pp. 566-569.

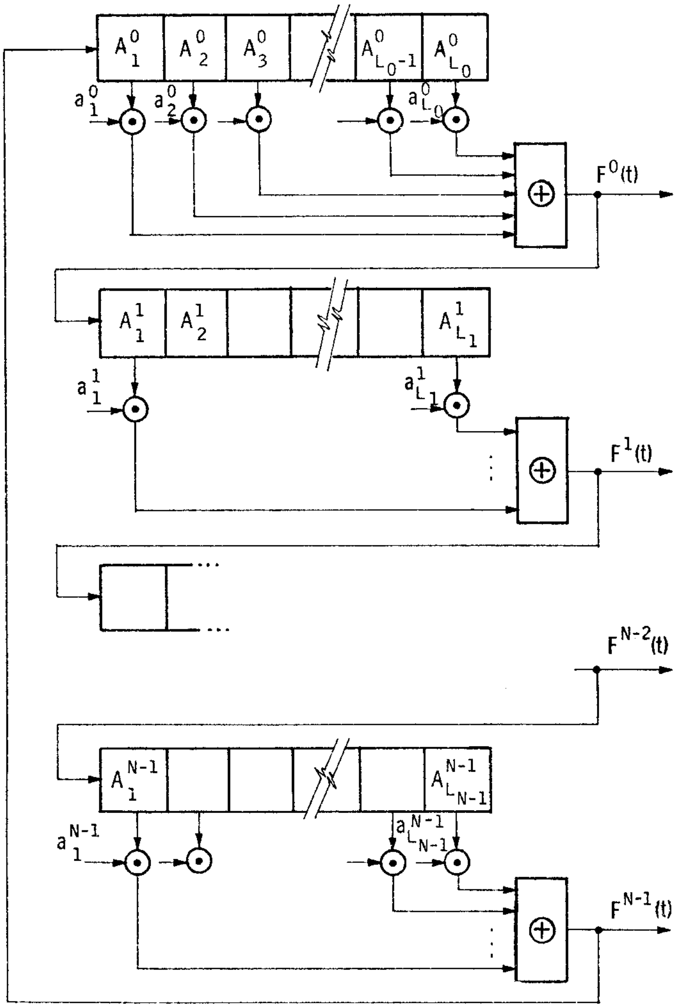
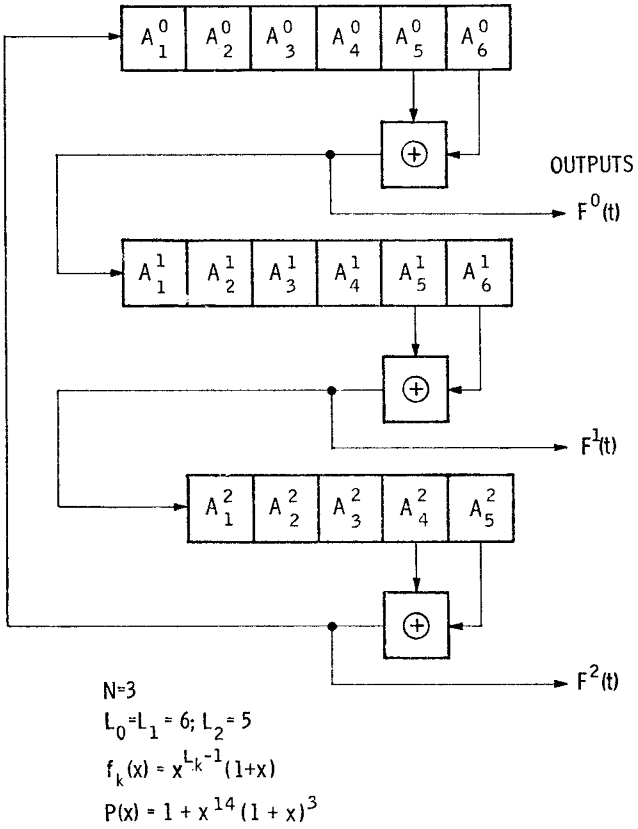


Fig. 1. A linear concatenation of *N* shift registers



A^0_1 A^0_2 A^0_3 A^0_4 A^0_5 A^0_6
OUTPUTS
$F^0(t)$
A^1_1 A^1_2 A^1_3 A^1_4 A^1_5 A^1_6
$F^1(t)$
A^2_1 A^2_2 A^2_3 A^2_4 A^2_5
$F^2(t)$
N=3
$L_0=L_1=6;\ L_2=5$
$f_k(x) = x^{L_k-1}(1+x)$
$P(x) = 1 + x^{14}(1+x)^3$

Fig. 2. An example concatenation with $b_k = 1$